acatech IMPULS

Digitale Souveränität

Status quo und Handlungsfelder

Henning Kagermann, Karl-Heinz Streibich,
Katrin Suder

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

acatech IMPULS

Digitale Souveränität

Status quo und Handlungsfelder

Henning Kagermann, Karl-Heinz Streibich, Katrin Suder

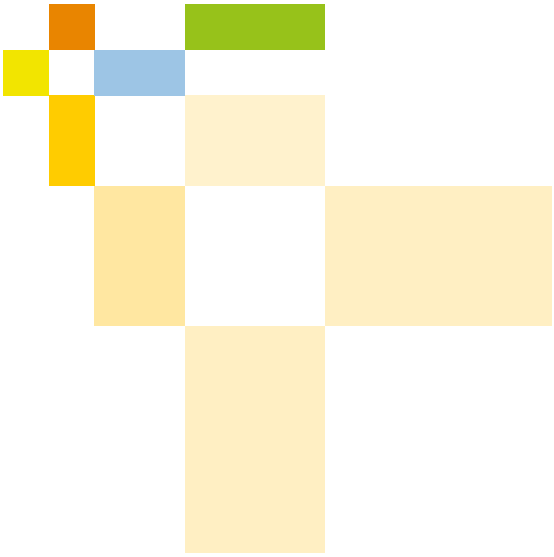
acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Die Reihe acatech IMPULS

In dieser Reihe erscheinen Debattenbeiträge und Denkanstöße zu technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Sie erörtern Handlungsoptionen, richten sich an Politik, Wissenschaft und Wirtschaft sowie die interessierte Öffentlichkeit. Impulse liegen in der inhaltlichen Verantwortung der jeweiligen Autorinnen und Autoren.

Alle bisher erschienenen acatech Publikationen stehen unter www.acatech.de/publikationen zur Verfügung.

Inhalt



Vorwort

Digitale Souveränität hat sich zu einer der entscheidenden politischen Zukunftsfragen entwickelt. Mit jedem neuen Bereich des privaten, wirtschaftlichen und öffentlichen Lebens, in dem wir digitale Plattformen und Anwendungen nutzen, wird Souveränität in der Nutzung entscheidender.

Digitale Souveränität ist nicht nur eine Frage der Wettbewerbsfähigkeit, sondern auch der politischen Selbstbestimmtheit der Europäischen Union und ihrer Mitgliedsstaaten, der Innovationskraft von Unternehmen und der Freiheit der Forschungseinrichtungen und aller Europäer in der digitalen Welt.

Digitale Souveränität europäischer Prägung muss dabei auf einen eigenständigen Weg der Digitalisierung abzielen. Weder staatliche Eingriffe und Abschottung im Sinne einer „Great Firewall" noch eine De-facto-Setzung entscheidender Normen durch Markmacht können Ziele sein. Die Idee einer Digitalen Souveränität europäischer Prägung zielt stattdessen auf eine Digitalisierung, die Wahlfreiheit lässt, die europäischen Rechts- und Wertevorstellungen folgt, die sich der Welt öffnet und fairen Wettbewerb fördert.

In seiner Präsidentschaft im Rat der Europäischen Union hat sich Deutschland für Digitale Souveränität als Leitmotiv der europäischen Digitalpolitik stark gemacht. Diese Notwendigkeit einer strategischen Befassung auf europäischer Ebene wurde jüngst in einem gemeinsamen offenen Brief der Bundeskanzlerin und der Regierungscheffinnen Dänemarks, Estlands und Finnlands an die Kommissionspräsidentin nochmals unterstrichen. Mit dem GAIA-X-Projekt haben europäische Vorreiter bereits die Grundlage für die Standardisierung einer vertrauenswürdigen europäischen Dateninfrastruktur auf Basis europäischer Wertvorstellungen und Grundrechte geschaffen.

Die Ausarbeitung einer konkreten Strategie, um diese gemeinsame europäische Vision Digitaler Souveränität zu erreichen, wird eine Gratwanderung sein: Es braucht praktische Lösungen, technologischen Abhängigkeiten im digitalen Raum zu begegnen und zugleich Wohlstand durch internationale Zusammenarbeit und globale Arbeitsteilung zu fördern.

Mit dem vorliegenden IMPULS wollen wir – gemeinsam mit vielen Expertinnen und Experten, die ihr Wissen und ihre Perspektiven eingebracht haben – zur konkreten Definition europäischer Digitaler Souveränität und zur Entwicklung konkreter Handlungsoptionen entlang der sie prägenden technologischen Ebenen beitragen.

Prof. Dr. Henning Kagermann

Karl-Heinz Streibich

Dr. Katrin Suder

Mitwirkende

Autorin und Autoren

- Prof. Dr. Henning Kagermann
- Karl-Heinz-Streibich
- Dr. Katrin Suder

Koordination und Redaktion durch acatech Geschäftsstelle

- Florian Süssenguth
- Dr. Johannes Winter

Mit Unterstützung durch acatech Geschäftsstelle

- Juliane Abdeen
- Dr.-Ing. Patrick Bollgrün
- Alexander Grieß
- Dr. Jorg Körner
- Dr. Martina Kohlhuber
- Peter Kraemer
- Dr. Annka Liepold
- Joachim Sedlmeir
- Christoph Uhlhaas
- Sebastian Witte

Interviewpartnerinnen und Interviewpartner

- Adel Al-Saleh, T-Systems International GmbH
- Dr.-Ing. Michael Bolle, Robert Bosch GmbH
- Sanjay Brahmawar, Software AG
- Dr. Svend Buhl, NXP Semiconductors
- Dr. Vanessa Cann, KI Bundesverband e. V.
- Mike Cosse, SAP SE
- Martin Fassunge, SAP SE
- Peter Ganten, Univention GmbH
- Dr. Norbert Gaus, Siemens AG
- Lisa Gradow, Bundesverband Deutsche Startups e. V.
- Prof. Dietmar Harhoff, Ph. D, MPI für Innovation und Wettbewerb
- Dr. Ralf Herbrich, Zalando SE
- Dr. Stefan Hofschen, Bundesdruckerei GmbH
- Dr.-Ing. Stefan Joeres, Robert Bosch GmbH
- Torsten Küpper, Qualcomm Technologies Inc.
- Rafael Laguna de la Vera, Bundesagentur für Sprunginnovationen
- Dr. Jürgen Müller, SAP SE
- Claudia Nemat, Deutsche Telekom AG
- Prof. Dr.-Ing. Boris Otto, Fraunhofer-Institut für Software- und Systemtechnik ISST und TU Dortmund
- Manfred Paeschke, Bundesdruckerei GmbH
- Prof. Dr. Peter Parycek, Fraunhofer FOKUS
- Dr.-Ing. Reinhard Ploss, Infineon Technologies AG
- Frank Riemensperger, Accenture GmbH
- Siim Sikkut, Ministerium für Wirtschaft und Kommunikation der Republik Estland
- Dr. Peter van Staa, Robert Bosch GmbH
- Joe Sullivan, Cloudflare Inc.
- Dr. Claudia Thamm, Bundesdruckerei GmbH
- Prof. Dr. Wolfgang Wahlster, DFKI
- Prof. Dr. Michael Waidner Fraunhofer SIT
- Arne Weber, IMS Evolve Ltd.
- Dr. Richard Weber, Cliqz MyOffrz GmbH
- Oliver Zipse, BMW AG

Weiterer Input

- BASF SE
- micro resist technology GmbH

Der vorliegende acatech IMPULS gibt die aus den Gesprächen gewonnenen Positionen und Bewertungen wieder, womit aber nicht ausgeschlossen soll, dass einzelne Interviewpartnerinnen und -partner zu bestimmten Fragen andere Standpunkte vertreten.

1 Digitale Souveränität für Deutschland und Europa

1.1 Definition und Bedeutung Digitaler Souveränität

Digitalisierung verändert ganze Branchen. Durch digitale Technologien und Dienste entstehen völlig neue Märkte. Während die USA und China in der konsumentennahen Plattformökonomie einen deutlichen Vorsprung aufgebaut haben, ist der globale **Wettlauf im industriellen Sektor** noch nicht entschieden.

Um die eigene industrielle **Innovationsfähigkeit** zu sichern und angesichts schwelender internationaler **Handelskonflikte Freiheitsgrade** zu bewahren, muss in Deutschland und Europa eine Diskussion über Digitale Souveränität in kritischen Technologiefeldern geführt werden. Es gilt, einen **eigenen, neuen Weg im europäischen Kontext** auf Basis einer kohärenten Strategie zu verfolgen.

Digitale Souveränität meint die Fähigkeit von Individuen, Unternehmen und Politik, frei zu entscheiden, wie und nach welchen Prioritäten die digitale Transformation gestaltet werden soll. Dafür sind **drei Hebel** zentral:

1. **Geeignete Technologien und Daten müssen verfügbar sein**, entweder indem diese selbst beherrscht werden oder indem der Zugang zu diesen abgesichert ist, auch in Krisenzeiten.

2. **Unternehmen, öffentliche Einrichtungen und ausreichende Fachkräfte müssen die Kompetenzen besitzen**, digitale Technologien zu bewerten, zu überprüfen und einzusetzen.

3. **Der digitale Binnenmarkt der Europäischen Union** muss Unternehmen erlauben, auf digitalen Technologien beruhende Geschäftsmodelle, Produkte und Dienste erfolgreich zu skalieren. Dies erfordert darüber hinaus eine regulatorische beziehungsweise industriepolitische Begleitung, auch um systemische Nachteile wie zum Beispiel das Risikokapitalgefälle zu den USA oder auch beschränkte Marktzugänge in China zu kompensieren.

Das Ziel aller Maßnahmen sollte eine digital geprägte **Industrialisierung in Europa** und darauf aufbauend eine **globale Skalierung** der Technologien und damit neuer Wertschöpfung sein. Das würde auch dazu beitragen, die bekannte **Transferschwäche Europas** trotz erstklassiger Forschung zu überwinden.

Durch eine Bündelung der Ziele und Aktivitäten der relevanten Bereiche sollten digitale **Schlüsseltechnologien** zukünftig **bis zum höchsten Technology Readiness Level begleitet** werden.

Der europäische Rechtsrahmen sollte dabei nicht auf eine Abschottung gegenüber ausländischen Akteuren, etwa amerikanischen und chinesischen Hyperscalern, ausgerichtet sein. Vielmehr sollten globale **Technologieunternehmen zu europäischen Bedingungen eingebunden** werden – etwa mit Blick auf Cybersicherheit, Datenschutz und Persönlichkeitsrechte.

1.2 Fokus des Papiers: der Technologie- und Datenhebel

Dieses Impulspapier fokussiert **auf den Technologie- und Datenhebel**. Um Digitale Souveränität zu erreichen, sind jedoch **alle drei Hebel von zentraler Bedeutung**. Technologie(n) allein wird/werden global nicht erfolgreich sein. Globaler Erfolg setzt auch Bewertungs- und Anwendungskompetenzen sowie eine strategische regulatorische industriepolitische Begleitung voraus, die bestehende Nachteile bei von Europa ausgehenden Skalierungsanstrengungen kompensiert.

Um die Dimensionen Digitaler Souveränität deutlich zu machen und der **gestiegenen Bedeutung digitaler Ökosysteme** Rechnung zu tragen, schlägt das Papier ein **modernisiertes Technologie-Schichtenmodell** (siehe Abbildung 1) vor, das genauer als die übliche Einteilung in Mikrochips, Hardware und Software differenziert und weitere heute relevante Ebenen in den Gesamtkontext einordnet.

Die **Bewertung und Diskussion** des Grades Digitaler Souveränität bei einzelnen Technologien erfolgt **entlang der acht Ebenen**. Dabei wurden die im Sinne der gewählten Definition von Digitaler Souveränität **relevantesten**, machbarsten und aktuell mit dem **größten politischen Handlungsbedarf verbundenen Technologiefelder identifiziert**. Die im Schichtenmodell angeführten **Beispiele existierender Reallabore und Institutionen** können als **Anknüpfungspunkte** weiterer Arbeiten dienen.

1.3 Übergreifende Handlungsempfehlungen

Dieses Impulspapier versteht sich als **Ausgangspunkt für eine breite Diskussion Digitaler Souveränität**, indem es mit dem Schichtenmodell einen Handlungsrahmen einführt und **je Ebene einen ersten Durchstich** vorstellt.

Für eine umfassende Betrachtung der Digitalen Souveränität Deutschlands und Europas ist aber eine **systematisch vorgenommene Vertiefung** zu **einzelnen Ebenen** und zu den **beiden anderen Hebeln erforderlich**.

Durch technologische **Foresightprozesse** sollten außerdem möglichst frühzeitig **Felder identifiziert** werde, die künftig für die Digitale Souveränität relevant werden könnten. Gezielte **Maßnahmen** könnten auf dieser Grundlage zeitnah erfolgen.

Auf Basis einer ebenenorientierten Analyse wäre auch ein **Kompetenzmonitoring für solche Felder zu empfehlen**, in denen es auf das **Zusammenspiel mehrerer Technologien** auf unterschiedlichen, übereinander geschichteten Ebenen ankommt. Beispiele dafür gab es in den vergangenen Jahren viele, etwa:

- die **Strategie der amerikanischen Hyperscaler** im B2C-Bereich: Die Vormachtstellung der amerikanischen Hyperscaler bei Cloudinfrastrukturen (Ebene 3) begründet deren Dominanz auch bei Plattformen, Daten und teilweise Software (Ebenen 4, 5, 6), da sie auf der unteren Ebene Lock-in-Effekte erzeugen, die Nutzerinnen und Nutzer ebenenübergreifend an ihr Ökosystem binden.
- die **europäische Dateninfrastruktur GAIA-X**: Um das Ziel der Reduktion solcher Lock-in-Effekte und der Abhängigkeiten von amerikanischen und chinesischen Hyperscalern zu erreichen, soll durch das Setzen verbindlicher Standards für in- und ausländische Anbieter und durch die Sicherstellung von Interoperabilität und Portabilität eine offene, föderierte, sichere und vertrauenswürdige digitale Dateninfrastruktur auf Basis europäischer Werte für Europa geschaffen werden. Diese kann als Grundlage für ein digitales Ökosystem dienen.
- **Künstliche Intelligenz und autonome Systeme**: Neue Wertschöpfung im industriellen Bereich setzt die Beherrschung der gesamten Produktionskette für KI voraus – spezialisierte Hardware und Mikrochips, die Erzeugung und Aufbereitung von Daten, Algorithmen und Software, Sensorik und Aktorik.
- **Quantencomputing**: Nur durch den Erhalt einer starken Basis bei Komponenten und die Schaffung europäische Kapazitäten bei Hardware für Quantencomputer kann die zukünftige Wertschöpfung durch Software und Algorithmen abgesichert werden.[1,2]

Diese Beispiele zeigen die Bedeutung einer **Analyse gegenwärtiger Stärken und Verwundbarkeiten** je Ebene. Erst diese erlaubt eine strategische Regulation und **Industriepolitik zu Zukunftsthemen**. Breit angelegte **strategische Allianzen** mit anderen, für die Technologien des Schichtenmodells relevanten Staaten müssen Teil der Bemühungen um Digitale Souveränität sein, um einseitige und zu starke Abhängigkeiten von einzelnen Wirtschaftsräumen möglichst gering zu halten.

1.4 Zusammenfassung

Das **wichtigste Element** der Souveränität ist die **Gestaltungsfreiheit**. In der digitalen Welt bedeutet das: **Entscheidungs- oder Wahlfreiheit** für oder gegen eine Technologie.

Entscheidend ist die Möglichkeit, **zwischen mehreren Anbietern** zu wählen. **Protektionismus ist nicht der richtige Weg**, Digitale Souveränität wird durch möglichst viele prosperierende Angebote gesichert.

Dort, **wo es keine Wahlfreiheit gibt**, sind folgende übergreifende Strategien **zu empfehlen**:

- Technologien sollten nicht einfach nachgebaut, sondern mittels Investitionen in die jeweilige **nächste Generation** entwickelt und beherrscht werden.
- Lock-in-Effekte in einzelne Technologien sollten vermieden werden – über **offene Standards**, **Interoperabilität**, **Portabilität** und **Kommodifizierung**.
- **Strategische relevante Assets** Deutschlands und Europas in globalen Wertschöpfungsnetzen sollten gesichert werden – nicht über Abschottung, sondern über globales Wachstum.

Strategische Weichenstellungen für **Innovation, Zukunftsfähigkeit und Wohlstand** in Europa bedeuten damit in vielen Fällen auch eine Stärkung der Digitalen Souveränität.

1 | Vgl. Kagermann et al. 2020.
2 | Vgl. Buchenau et al. 2021.

2 Das Technologie-Schichtenmodell

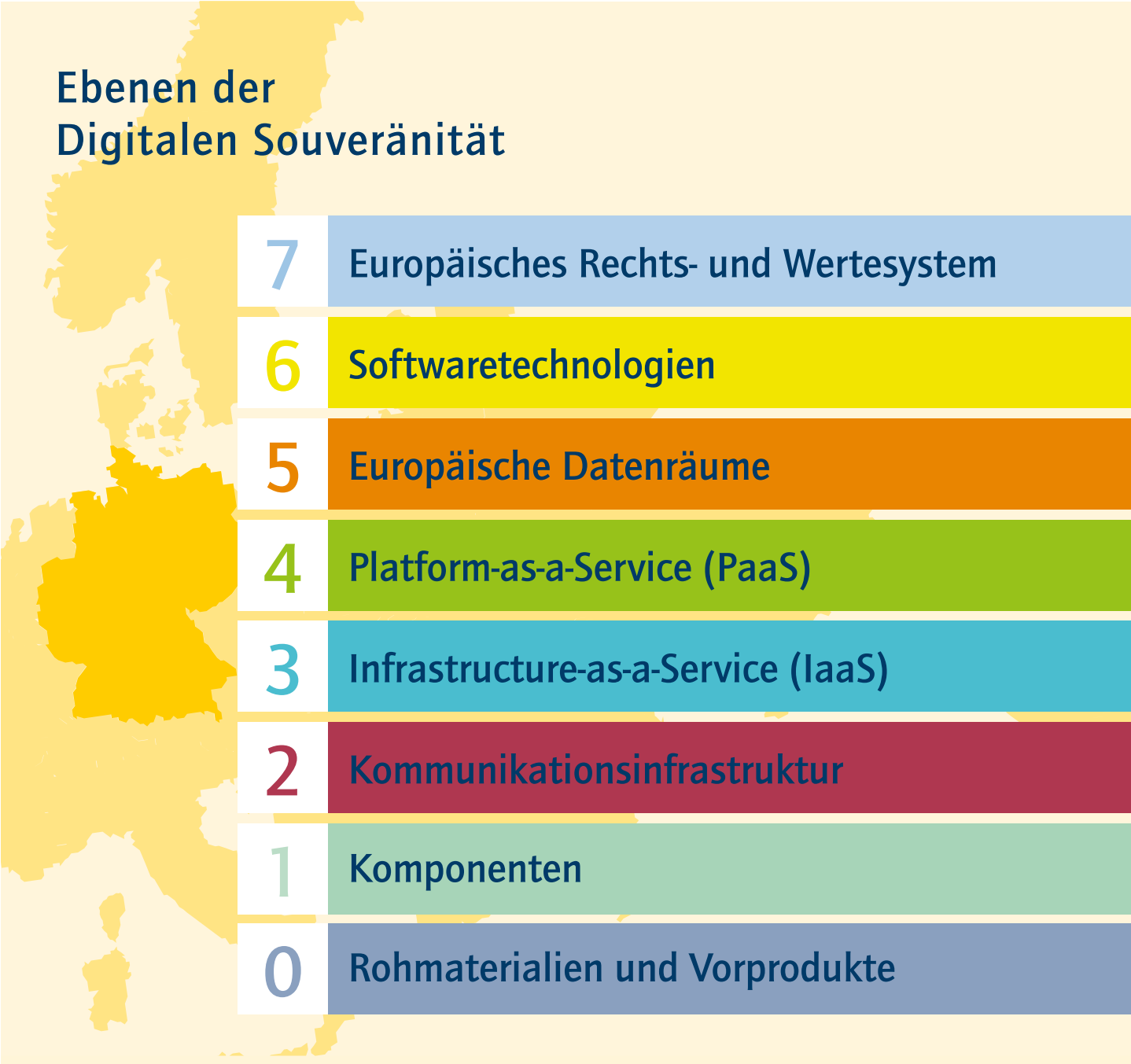


Abbildung 1: Schichtenmodell der aufeinander aufbauenden Ebenen der Digitalen Souveränität (Quelle: eigene Darstellung)

Bestandteile/Fokusbereich	Reallabore und Institutionen
Cybersecurity, Kryptografie, **E-Identity,** EU-Zertifizierung (Verbraucherschutz) und Standards	Reallabor: Cybersecurity Center Institution: BSI + Netzwerk Cyberregionen in D
App-Entwicklungen, Office, ERP, KI, Middleware, Robotik-Software, Blockchain, Algorithmen, **EU-Open Source,** VR/AR, QC	Reallabor: keines Institution: Agentur für Sprunginnovation, KI-Verbund
Zum Beispiel für **Mobilität**, Health, Public Sector, digitaler öffentlicher Raum	Reallabor: Datenraum Mobilität Institution: GAIA-X, Datenstrategie D, EU
Anwendungs- und Entwicklungsökosysteme B2B und B2C (Abstraction Layer, Container Technology) QC, KI, **IoT**	Reallabor: keines Institution: GAIA-X/Vollendung des europäischen Binnenmarkts
Virtuelle, verteilte Cloud-Ökosysteme, Edge-Technologie, QC, KI-HPC-Center	Reallabor: **Gardener** (Deutsche Telekom, SAP, Bosch ...) Institution: GAIA-X
Breitbandinfrastruktur, Mobilfunknetze **(Open RAN)**, Galileo-Navigation	Reallabor: **Open RAN** Institution: O-RAN Alliance
Mikrochips, Sensoren, Aktuatoren, Fertigungs- und Basistechnologien, 3D-Druck, QC, KI	Institution: IPCEI Mikroelektronik
Seltene Erden ...	Institution: Rohstoffagentur (BMWi)

0 Rohmaterialien und Vorprodukte

Seltene Erden ... | Institution: Rohstoffagentur (BMWi)

Elemente dieser Ebene

Diese Ebene umfasst das sehr **heterogene Feld der Rohmaterialen und Vorprodukte**, die für die Produktion elektronischer Komponenten wie beispielsweise Mikrochips und Batterien benötigt werden. **Seltene Erden** sind das bekannteste Beispiel für Ressourcen, die in modernen Geräten unerlässlich sind. Ebenso wichtig sind beispielsweise auch hochreine und hochwertige **Prozesschemikalien**, die im Fertigungsprozess eingesetzt werden.

Darüber hinaus wächst die Nachfrage nach neuartigen **Hightech-Rohstoffen**. Ein Beispiel für letztere sind **funktionalisierte Materialien** wie Quantenpunkte, deren Absorptions- und Emissionseigenschaften durch die Wahl der Partikelgröße und Manipulation der Partikeloberfläche präzise angepasst werden können.

Status quo

Bei vielen Rohstoffen und Vorprodukten hat in den letzten Jahrzehnten eine **Verlagerung der Wertschöpfungsnetzwerke nach Asien** stattgefunden. Gründe hierfür liegen neben **Kostenvorteilen** auch in der **Nähe zu wichtigen Kunden**, mit denen gemeinsam Innovationen vorangetrieben werden, sowie einer umweltschonenden Verkürzung von Transportwegen.

Die daraus resultierende, **allgemein zunehmende Abhängigkeit** europäischer Hersteller von den amerikanischen und asiatischen Rohmaterial- und Vorprodukteanbietern stellt **insbesondere KMU vor große Herausforderungen**, die aufgrund ihrer begrenzen Marktmacht nur wenig Einfluss auf Rahmenbedingungen nehmen können.

Lösungsansatz

Autonomie ist auf dieser Ebene **nicht erreichbar**. Die bestehenden **Abhängigkeiten** lassen sich durch verschiedene Maßnahmen adressieren, die im Rahmen einer **aktualisierten Rohstoffstrategie** gebündelt werden könnten:

- **Kontinuierliches Monitoring** des Rohstoffbedarfs und der Rohstoffverfügbarkeit durch die **Deutsche Rohstoffagentur**; gegebenenfalls Ausweitung des Monitorings auf komplexere Vorprodukte
- **Politische Initiativen** zur Absicherung des Zugangs zu Rohstoffen und Vorprodukten mit nur einem Anbieter sowie zur Steigerung der Unabhängigkeit, zum Beispiel durch Erschließen einer zweiten Rohstoffquelle oder einer Förderung des Aufbaus von Produktionskapazitäten für Prozesschemikalien
- Verstärkter Einsatz der **Circular Economy** zur **Senkung des Importvolumens** einiger Rohstoffe und **Förderung der Forschung zu Substitutionsmöglichkeiten** für knappe Rohstoffe

Zusammenfassung

Die europäische Wirtschaft wird dauerhaft von Rohstoffimporten abhängig bleiben. Kritische Abhängigkeiten lassen sich nur durch kontinuierliches **Monitoring**, **vorausschauendes Handeln** und die **Entwicklung von Alternativen** vermeiden. Bei Hightech-Rohstoffen wäre darüber hinaus die Schaffung gegenseitiger Abhängigkeiten denkbar.

1 Komponenten

Mikrochips, Sensoren, Aktuatoren, Fertigungs- und Basistechnologien, 3D-Druck, QC, KI

Institution: IPCEI Mikroelektronik

Elemente dieser Ebene

Die Komponentenebene umfasst **Mikrochips, Sensoren, Aktuatoren**. Als Grundlage aller weiteren Infrastrukturen haben diese **Komponenten**, die für sie benötigten **Basis- und Fertigungstechnologien** sowie teilweise auch Entwicklungs-Softwaretools eine besondere Bedeutung, zumal sie zunehmend ins **Zentrum geopolitischer Konflikte** rücken, insbesondere zwischen den USA und China.

In der **Sensorik, der Aktorik und den Fertigungstechnologien** ist Deutschland mit am Standort etablierten Firmen gut aufgestellt. Es kann auch eine Reihe von Start-ups vorweisen, zum Beispiel Q.Ant (Quantensensorik) und Franka Emika (Robotik). Forschungszentren für technische Grundlagen der Mensch-Maschine-Interaktion wurden gegründet beziehungsweise ausgebaut. Hinsichtlich der Digitalen Souveränität gilt es daher, diese **Stärken aufrechtzuerhalten**.

Fokusbereich Mikrochips – Status quo

	Bedeutung für Digitale Souveränität	Grad der Abhängigkeiten außerhalb der EU	Grad der resultierenden Verwundbarkeit
Funktionale Ebene (Produkt als Funktionsobjekt an sich, ohne Fertigung)			
Prozessoren für KI, Datenverarbeitung, Kommunikation (4G/5G)			
Speicher			
Sensorik			
Leistungselektronik			
Designebene (Fähigkeit zur Entwicklung der Produkte der funktionalen Ebene)			
Grundlegende Design-Softwaretools (CAD) für Schaltungsentwicklung			
Ergänzende Entwicklungssoftware			
Fertigungs- und Basistechnologien (Voraussetzung für Fertigung der Produkte der funktionalen Ebene)			
Chipfertigung – hochintegrierte Produkte			
Chipfertigung – Sensorik und Leistungselektronik			
Packaging und Test			
Fertigungsequipment (spezialisierte Anlagen, Maschinen)			
Equipment für Chipproduktion			
Equipment für Packaging			
Testequipment			

Bedeutung der Farbwerte

Niedrig — Hoch

Abbildung 2: Heatmap Technologiefeld Mikrochips: hinsichtlich Digitaler Souveränität zu priorisierende Teilbereiche, in diesen bestehende Abhängigkeiten und aus gegenwärtiger Struktur des jeweiligen Teilbereichs resultierende Verwundbarkeiten (Quelle: eigene Darstellung)

Politischer Handlungsbedarf besteht auf dieser Ebene stattdessen vor allem im Bereich **Mikrochips**.

Hier zeigt sich ein **sehr gemischtes Bild**. Das Feld zeichnet sich durch oftmals weitverzweigte internationale Lieferketten und dadurch einen hohen Grad an **Abhängigkeiten von Wirtschaftsräumen jenseits der EU** aus. Daraus resultieren je nach Teilgebiet unterschiedlich hohe **potenzielle Verwundbarkeiten** (siehe Abbildung 2). Im ersten Quartal des Jahres 2021 wurden diese Verwundbarkeiten durch eine konkrete Mangelsituation in zahlreichen Branchen deutlich sichtbar.

Da ein Aufholen in allen Bereichen gleichermaßen unwahrscheinlich ist und volkswirtschaftlich ineffizient wäre, stellt sich die Frage, in welchem Bereich Europa **Kompetenzen und Kapazitäten auf- und ausbauen** sollte. Diese sollten sowohl der Digitalen **Souveränität der heimischen industriellen Basis** zugute kommen als auch **international als Verhandlungsmasse** genutzt werden können.

- **High-End-Mikrochips:** Die **etablierte technologische Abhängigkeit** bei High-End-Mikrochips auf Basis von Fertigungsverfahren mit einer Auflösung von fünf Nanometern und weniger (More Moore) ist **nicht mehr ohne Weiteres zu lösen**. Lediglich TSMC (Taiwan) und Samsung (Südkorea) sind in der Lage, solche High-End-Chips zu produzieren. Bei ihrem Einsatz erlauben ihre Überprüfung und die Verschlüsselung der verarbeiteten Daten aber eine gewisse Souveränität.
  Auch bei der **Chipfertigung für hochintegrierte Produkte** greifen Unternehmen gegenwärtig vor allem auf Taiwan und Südkorea zurück. In Deutschland bestehen hierfür nur **in Teilen Kompetenzen bei Basistechnologien** und nur **wenig Fertigungstechnikkompetenzen**.
  Die führenden **Chiphersteller** sind allerdings selbst wiederum **von einer europäischen Firma abhängig.** ASML (Niederlande) ist mit einem Zwei-Drittel-Marktanteil der weltgrößte Anbieter von Lithografiesystemen, die für die Chipfertigung essenziell sind. Zeiss und Trumpf sind wiederum wichtige Zulieferer für ASML. Diese europäischen Firmen stellen damit eine gewisse Machtstelle beziehungsweise einen **Schutzschirm im weltweiten Lieferkettensystem** für High-End-Chips dar.
- **Spezialisierte Mikrochips**: Für viele Vorhaben in **Zukunftsfeldern** der industriellen Wertschöpfung in Deutschland wie IoT und Edge-Computing, stationäre Mobilfunkstationen und Branchen wie den Automobilbau und die Pharmaindustrie sind auf reine Leistung optimierte **High-End-Chips aber nicht notwendig**.
  Entscheidender sind oftmals **niedrige Kosten** und Eigenschaften wie ein **niedriger Energieverbrauch, hohe Lebensdauer** oder **spezialisierte Funktionen**. Diese lassen sich auch mit **„Good-Enough"-Fertigungsverfahren** zwischen 12 und 28 Nanometern verwirklichen. Dies gilt sogar für hochinnovative Ansätze wie siliziumbasierte Photonikchips für das Quantencomputing.
  Jedoch ist **Europa auch hier nicht souverän**, da in diesem Bereich **keine ausreichenden Fertigungskapazitäten** in europäischer Hand liegen. **Globalfoundries** bietet in Dresden zwar die Fertigung auf zwanzig Nanometern an, produzierte aber in den vergangenen Jahren **am Bedarf der europäischen Industrie vorbei** und befindet sich im **Besitz von Abu Dhabi**.
  Die im Raum stehende **Übernahme von ARM Limited** durch die amerikanische NVIDIA Corporation stellt eine **Gefährdung der europäischen Digitalen Souveränität** dar. Eine Genehmigung der Übernahmepläne durch europäische Aufsichtsbehörden sollte daher deutliche Auflagen beinhalten, mit denen sowohl der Zugang zu wichtigem **geistigen Eigentum** als auch **Know-how zu Chipsegmenten** erhalten bleibt, die für **eingebettete Systeme und vernetze Geräte** relevant sind.

Während also Investitionen in den Versuch, im reinen More-Moore-Bereich aufzuholen, wenig sinnvoll erscheinen, kann der politisch unterstütze **Aufbau von Kapazitäten** im Design und in der Fertigung **spezialisierter Chips** (**More Than Moore**) und neuartiger Chips auf Basis innovativer Materialien, Architekturen, dreidimensionaler Strukturen oder Fertigungstechnologien (**Beyond Moore**) **lohnen**.

Wichtig hierfür ist es auch, Standards zu setzen und **innovative Produktkategorien zu definieren**, wofür eine entsprechende **Nachfrage aus Leitindustrien nötig** ist. Hierfür bestehen im Mobilfunkbereich (Nokia, Ericsson) und im Fahrzeugbau gute Ausgangslagen. Der Maschinenbau dagegen nutzt bislang typischerweise Produkte, die an anderer Stelle definiert wurden.

Lösungsansatz

Eine **Ausweitung politischer Vorhaben** zur Stärkung der für viele industrielle und digitale Zukunftsfelder Deutschlands und Europas wichtiger werdenden Mikrochipbasis wäre nötig, da das **aktuelle Niveau** eine weitere **Verschlechterung der Position** im Gewebe wechselseitiger Abhängigkeiten befürchten lässt.

Im Folgenden werden **drei Ansatzpunkte** für eine politische Stärkung des Feldes vorgestellt:

- **Marktentwicklung**: Die europäischen Hableiter- und Mikrochiphersteller sind darin zu bestärken, zukünftig **relevante Mikrochip- und Produktionstechnologien** zu identifizieren und dadurch entstehende Machtstellen durch einen **schnellen Markteintritt** zu besetzen. Dies kann nur gelingen, wenn sich hier auch **Leitindustrien** abseits von Automotive und Mobilfunk **aktiver einbringen**.
  Die genauen Richtungsentscheidungen sind zwar grundsätzlich dem Markt zu überlassen – eine **Flankierung durch industriepolitische Instrumente** kann aber Durchbrüche erleichtern.
  Eine **strategisch geleitete öffentliche Beschaffung** könnte hier starke Impulse setzen. Zu **weiteren relevanten Maßnahmen** gehören unter anderem der Schutz vor ausländischen Übernahmen, eine verstärkte europäische Konsolidierung, die gezielte Förderung von Sprunginnovationen oder auch das Engagement der Ministerien und Behörden in Standardisierungsgremien.
  Der **strategische Bezugsrahmen** für Entscheidungen über den Einsatz von Beihilfeinstrumenten muss zukünftig der **globale Markt**, nicht wie bisher der europäische Binnenmarkt sein.
- **Mikroelektronik-IPCEI**: Das IPCEI gilt es in der **nächsten Phase zu stärken**. Dies beinhaltet eine ausreichende **Ressourcenausstattung** und eine deutliche **Beschleunigung** der Entscheidungsverfahren.
- **Neue Foundry im 20-bis-60-Nanometer-Bereich**: Der Aufbau einer solchen Foundry **in europäischer Hand**, beispielsweise im Rahmen eines **weiteren IPCEI**, sollte geprüft werden. Durch eine derart abgesicherte, **gezielte Versorgung** mit den für die deutsche und europäische Industrie **zentralen Chiptypen** könnte die Weiterentwicklung des Ökosystems gestützt werden.
  Ein solches Vorhaben kann auf **bestehenden Initiativen** und den Unternehmen aufbauen, die bereits im ersten IPCEI Erfahrungen gesammelt haben. Das mittelfristige **Ziel** muss eine unternehmerisch getriebene, nach einer Phase öffentlicher Förderung durch die EU oder einen Zusammenschluss einzelner EU-Mitgliedsstaaten **international wettbewerbsfähige** Fertigung **maßgeschneiderter Chips** sein.

Zusammenfassung

Statt ein aufwendiges Aufholen im More-Moore-Bereich anzustreben, sollten Stärken bei spezialisierten **More-than-Moore-Chips** auf- und ausgebaut werden und **Vorsprünge** im Wettlauf um **neuartige Beyond-Moore-Chiptechnologien** erreicht werden. Diese können dann im durch starke wechselseitige internationale Abhängigkeiten geprägten Feld der Mikrochips für Europa **als „Verhandlungsmasse"** verstanden und in einem Eskalationsszenario auch eingesetzt werden, um wiederum den Zugang zu anderen, nicht in Europa produzierten Chiptypen abzusichern.

2 Kommunikationsinfrastruktur

Breitbandinfrastruktur, Mobilfunknetze **(Open RAN)**, Galileo-Navigation

Reallabor: **Open RAN**
Institution: O-RAN Alliance

Elemente dieser Ebene

Für die Ebene der Kommunikationsinfrastruktur werden **Breitbandinfrastruktur** (Fest- und terrestrische Mobilfunknetze) sowie **satellitengestützte Navigation** als kritische Bereiche identifiziert.

Das **Mobilfunknetz** setzt sich aus **Zugangsnetz** (Antennen und deren Steuerung), **Transport-**, **Aggregations-** und **Kernnetz** zusammen. Während über siebzig Prozent der Investitionen auf das Zugangsnetz entfallen, hat das **Kernnetz** die **höchste Sicherheitskritikalität**. Diese Kritikalität beruht auf der Tatsache, dass über das Kernnetz die **Verkehre gemanagt**, das **Netz gesteuert** und die **Metadaten verwaltet** werden.

Alle Netzbereiche basieren heute auf **Technologiekomponenten** unterschiedlicher europäischer, amerikanischer und chinesischer beziehungsweise asiatischer Hersteller (zum Beispiel Ericsson, Nokia, Cisco, Juniper, Microsoft, Huawei, Samsung). Während in Europa weit über hundert Mobilfunkanbieter existieren, ist die **Anzahl** der weltweit zur Verfügung stehenden **Technologielieferanten** pro **Kategorie** sehr **klein**. Das gilt insbesondere für das **mobile Zugangsnetz**. Hier haben Huawei, Ericsson und Nokia einen Marktanteil von über 75 Prozent. Dadurch ergeben sich **technologische Abhängigkeiten**, die nicht leicht zu lösen sind – auch wenn die einzelnen Komponenten durch die großen Telekommunikationsanbieter weitgehend souverän eingebaut, verwaltet und gesteuert werden.

Im Bereich der **satellitengestützten Navigation** ist das europäische globale System **„Galileo"** zu nennen, das als **unabhängige** und **zivile Alternative** zum US-amerikanischen NAVSTAR-GPS, dem russischen GLONASS-System und dem chinesischen Beidou-System fungiert. Die **Einsatzfähigkeit** von Galileo muss zum Erhalt der technologischen Souveränität auf diesem Gebiet gesichert sein.

Im Folgenden wird speziell auf die Fragestellung eingegangen, wie die **Lieferantenvielfalt** vergrößert werden kann, um damit auch **Innovationen** für die **mobilen Zugangsnetze** zu forcieren.

Fokusbereich Mobilfunkzugangsnetze – Status quo

Die **Mobilfunkzugangsnetze** („Radio Access Networks") bestehen aus den **technischen Komponenten** a) Funkzelle mit Antenne, b) Funkeinheit/Radio Unit, c) Basiseinheit/Baseband Unit. Sie sind typischerweise nur von **jeweils einem der wenigen dominanten Netzausrüster** integriert und beinhalten **proprietäre, nicht interoperable Technologien**.

Aktuell beherrscht **Huawei** den **Weltmarkt**. **Alternative** Ausrüster aus **Europa** sind **Ericsson** und **Nokia**, jedoch verwendet jedes dieser drei Unternehmen **proprietäre Standards**. Dies führt zu unerwünschten **Lock-in-Effekten**, **hemmt** die **Innovationskraft** und **reduziert** die **Flexibilität** bei der Umstellung auf aktuelle und zukünftige Mobilfunkstandards (5G, 6G).

Lösungsansatz

Potenziell negativen Konsequenzen für die technologische Souveränität aufgrund von Lock-in-Effekten infolge der Konzentration auf wenige Hersteller wird mit dem Ansatz **O-RAN** (Open Radio Access Network) über eine **standardisierte** und **offene Netzwerkarchitektur** für das Mobilfunk-Zugangsnetz begegnet.

Wenn die Komponenten Antenne, Radio Unit und Baseband Unit verschiedener Hersteller einem **gemeinsamen O-RAN-Standard** folgen und über **offene Schnittstellen** kommunizieren, könnten deutlich höhere Flexibilität, geringere Abhängigkeiten von wenigen dominanten Netzausrüstern und ein **erleichterter Markteintritt** neuer, auch **kleinerer** weiterer **europäischer Anbieter** erreicht werden. Infolgedessen werden mehr **Innovationen** und aufgrund höherer Transparenz und Kontrolle ein höheres **Sicherheitsniveau** im Netz ermöglicht (siehe Abbildung 3).

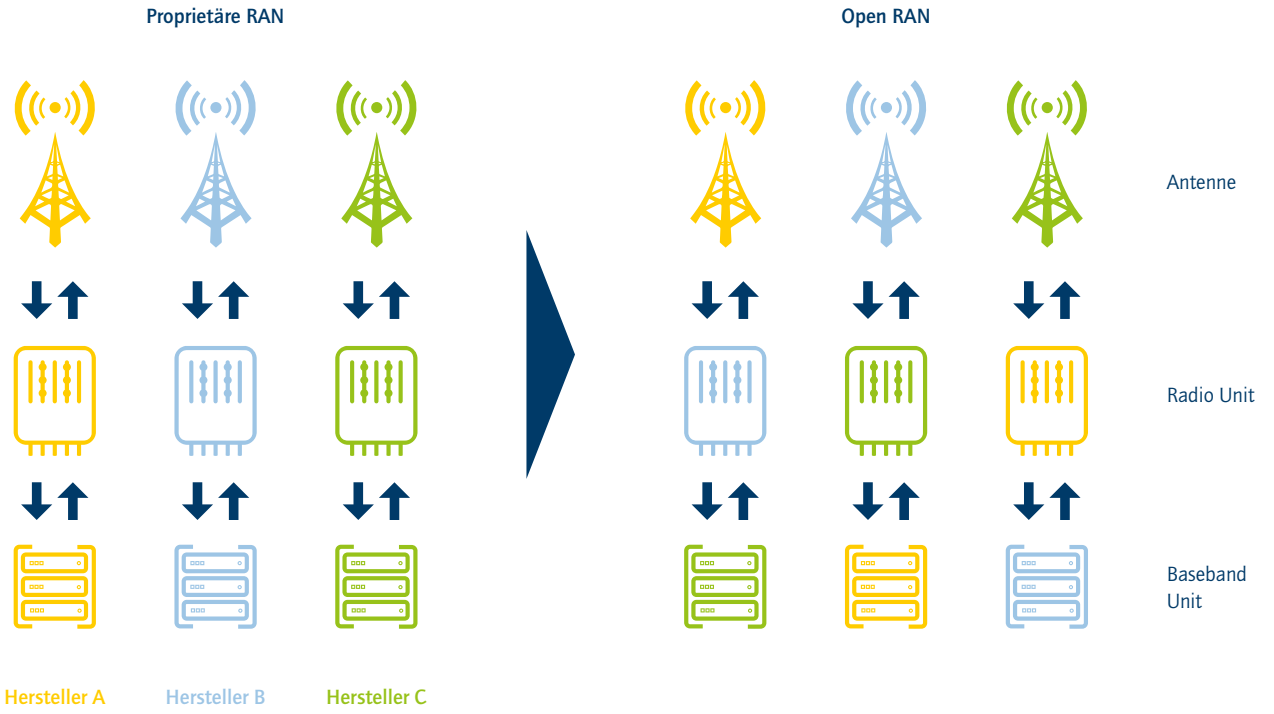


Abbildung 3: Übergang vom Status quo hin zur standardisierten und offenen Netzwerkarchitektur des O-RAN-Ansatzes (Quelle: eigene Darstellung auf Basis von Telefónica Deutschland 2020)

In der globalen **O-RAN Alliance** arbeiten mehrere **weltweit führende Netzbetreiber** zusammen an den erforderlichen **Spezifikationen**. Auch die großen europäischen Netzausrüster sind hier – neben zahlreichen, auch kleineren Tech-Unternehmen – beteiligt, allerdings bestehen auch hier noch signifikante Abhängigkeiten von einzelnen Anbietern, beispielsweise Intel.

Allerdings ist bei allein circa 30.000 bestehenden Antennenstandorten der Deutschen Telekom die Einführung von Open-RAN-kompatiblen Netzkomponenten nur **schrittweise realisierbar** und eine **Offenlegung** der bereits verbauten **Schnittstellen** und **Protokolle** Voraussetzung für die Weiternutzung **bestehender Komponenten** in einer **Open-Ran-Architektur**.

Dazu müssen die aktuell dominanten Hersteller **kooperieren**. Daher und aufgrund der **Komplexität** der Netze ist davon auszugehen, dass ein solcher **Umbau** sich über **viele Jahre** erstrecken wird. Um diesen Prozess zu beschleunigen, sollten **vollständig offene Implementierungen** der drei Schichten gefördert werden. Die DARPA ist einen solchen Schritt jüngst zusammen mit der Linux-Foundation gegangen, ein Vorschlag der Bundesagentur für Sprunginnovationen (SprinD) liegt seit November 2020 vor.

Generell gilt es auch weiterhin zu prüfen, wie der **europäische Telekommunikationsmarkt** systemisch über **industriepolitische Maßnahmen** und **regulatorische Vorgaben** beziehungsweise **Mechanismen** strukturell verbessert werden kann. Dabei sollte eine Fokussierung beziehungsweise Ausrichtung auf die **europäischen Anbieter** (Nokia, Ericsson und andere) erfolgen, um ihre **Wettbewerbsposition** insbesondere gegenüber den Akteuren aus den USA und Asien **strategisch** und **nachhaltig** zu **stärken**.

Zusammenfassung

Bei den **Mobilfunk-Zugangsnetzen** besteht durch eine **fehlende vertikale Kompatibilität** der verschiedenen Komponenten eine **Abhängigkeit** von **wenigen Herstellern**. Um dieser Entwicklung gegenzusteuern, hat die **O-RAN Alliance** das Ziel, **offene Schnittstellen** zu etablieren. Ein vollständig offener Open-Source-Ansatz würde **Innovation** (zum Beispiel 6G), **Wettbewerb**, **Resilienz** und **Transparenz** im Bereich Mobilfunk fördern.

Innerhalb des **europäischen Telekommunikationsmarktes** ist es wichtig, über geeignete **industriepolitische Maßnahmen** und **regulatorische Ansätze** die Position der **europäischen Anbieter** zu **verbessern**.

3 Infrastructure-as-a-Service (IaaS)

Virtuelle, verteilte Cloud-Ökosysteme, Edge-Technologie, QC, KI-HPC-Center

Reallabor: **Gardener** (Deutsche Telekom, SAP, Bosch …)
Institution: GAIA-X

Elemente dieser Ebene

Diese Ebene beinhaltet Hardware und Systemsoftware und bildet dadurch die technologische Basis der Vernetzung (**connect**), der Bereitstellung von Rechenkapazität (**compute**) sowie der Speicherung von Daten auf Servern (**store**).

In den traditionellen Bereichen (zum Beispiel Rechenzentren) ist die Hardware eine verfügbare, standardisierte Commodity. Anwender von Geschäftssoftware oder Ähnlichem können die erforderliche Hardware wie PCs und Notebooks **frei wählen** und damit **Abhängigkeiten** von einzelnen Herstellern **vermeiden**. Solange **Hardware und Software entkoppelt sind**, fällt es nicht ins Gewicht, dass es im privaten und kommerziellen Bereich keine nennenswerten deutschen Hardwareanbieter gibt. Mit dem Aufkommen der Cloud **verlieren** die Anwenderunternehmen diese **Souveränität**. Sie werden zu **Konsumenten** technischer Cloud-Dienste, die „**as a service**" von spezialisierten Anbietern betrieben und zur Verfügung gestellt werden. Hierdurch entwickeln sich **Netzwerk- und Skaleneffekte zugunsten der Anbieter von Cloud-Diensten** als zugrunde liegender Plattform. Aufgrund der immensen Investitionen durch die Notwendigkeit einer globalen Präsenz entstehen **Oligopol-Tendenzen** mit wenigen marktbeherrschenden **Cloud-Infrastruktur-Anbietern** (**Hyperscalern**) wie Microsoft, AWS oder Google, die einen **Lock-in** der Anwender auf diesen Plattformen anstreben. Dieser entsteht durch die **zwingende Verbindung** eben dieser wenig differenzierenden Cloud-Infrastruktur mit den Anwendungsplattformen (siehe PaaS, Ebene 4).

Den Cloud-Unternehmen ermöglicht dies den Aufbau riesiger **globaler Datenräume** (Ebene 5), die ihnen einen globalen Vorsprung bei innovativen Anwendungen – vor allem aber bei **KI/ Machine Learning** – verschaffen.

Die **Hyperscaler** sind im europäischen Raum bis auf Weiteres – auch im Falle einer erfolgreichen Umsetzung von GAIA-X – **nicht so schnell zu ersetzen**. Allerdings sind amerikanische Hyperscaler dem **US CLOUD Act** ausgesetzt, was auch die **Datensicherheit** der **in Europa** gespeicherten Daten **gefährdet**. Aus diesem Grund ist es geboten, **Kooperationen** mit ihnen nach **europäischem Recht in Europa** zu etablieren und parallel die eigenen Fähigkeiten und Angebote zu entwickeln.

Das **Projekt Sovereign Cloud Stack (SCS)** in GAIA-X hat genau dies zum Ziel: Es schafft ein **Netzwerk von Anbietern**, welche auf Basis von **gemeinsam und präzise definierten Standards**, freier Software und dokumentierten Betriebsprozessen föderierbare Infrastrukturdienste (IaaS/CaaS/PaaS) entwickeln und bereitstellen. Somit wird durch eine **Vielzahl von Anbietern** (und auch optionaler selbst betriebener Umgebungen) eine **hochgradig interoperable virtuelle Cloud** geschaffen.

Fokus der Entwicklungsbereiche für Europa: Portabilität und Standardisierung, virtuelle High-Performance-Computing(HPC)-Netzwerke und Next Generation Technologies

- **Portabilität und Standardisierung**: Viele moderne Workloads setzen auf der Containerebene auf und können mithilfe von Multi-Cloud Containerframeworks wie Rancher, Kubermatic oder Gardener unabhängig von der darunterliegenden IaaS-Schicht umgesetzt und betrieben werden. Dieses Abstrahierungslayer **entkoppelt die Anwendungsplattformen** von der Cloud-Infrastruktur und **durchbricht damit die Lock-In-Strategie der Hyperscaler** und macht Anwendungsplattformen portierbar. So können zum Beispiel Containerworkloads zwischen Hyperscalern und SCS-basierten, souveränen Clouds verschoben werden.
- Ein vielversprechender Ansatz ist hier das von der SAP und der Deutschen Telekom aufgesetzte und auf der Grundidee von GAIA-X basierende kommerzielle Open-Source-Projekt der **Gardener Cloud Foundation (GCF)**. Es hat die Schaffung eines digitalen Ökosystems auf Basis **offener Standards bei verteilten Systemen** zum Ziel (siehe Abbildung 4). Durch diese **Portierbarkeit der Anwendungsplattformen** kann die **Lock-in-Strategie** der **Hyperscaler** – im Interesse eines fairen Wettbewerbs – **unterlaufen** und **„Infrastructure-as-a-Service"** gegebenenfalls wieder zur **Commodity** werden. Verschiedene Anwender nutzen bereits GCF im Rahmen ihrer Multi-Cloud-Strategie.

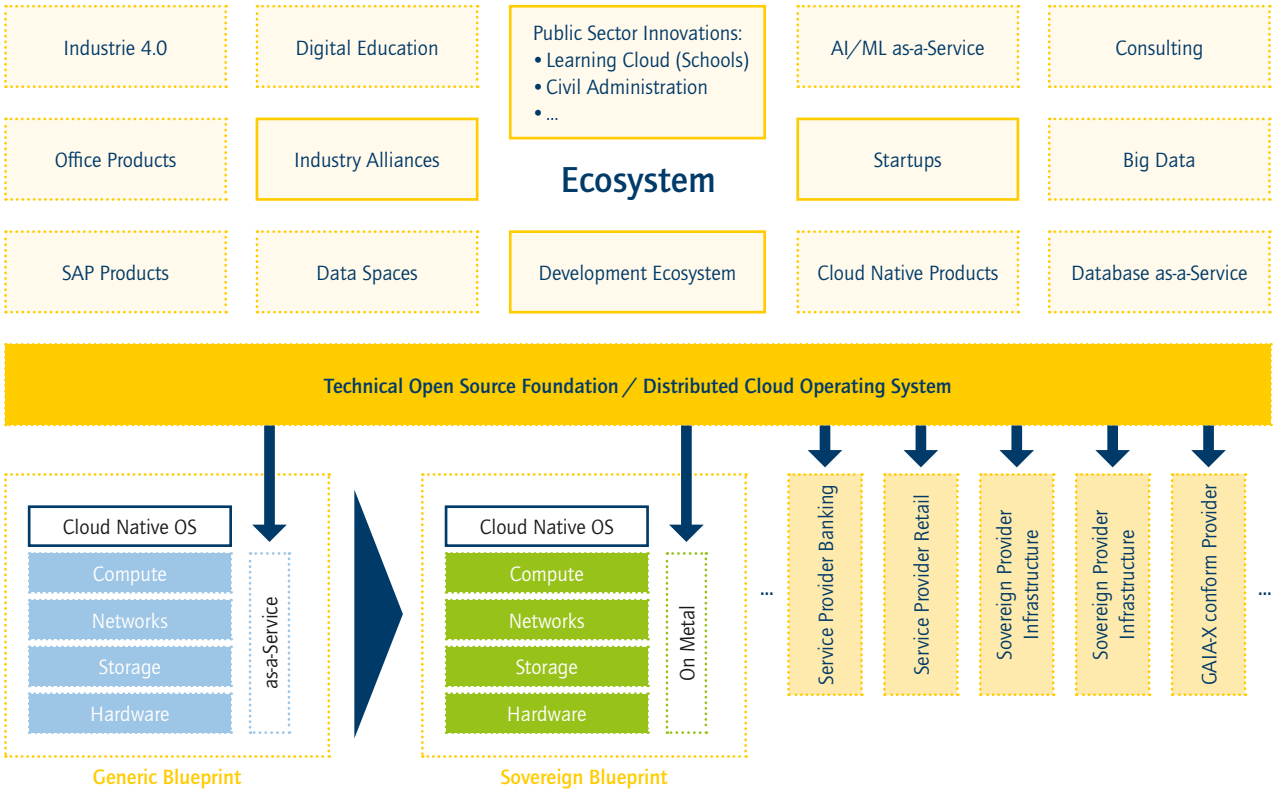


Abbildung 4: Gardener – ein offener, kohärenter und erweiterbarer Standard (Quelle: eigene Darstellung auf Basis von SAP 2021)

- **Virtuelle KI-High-Performance-Computing-Center (KI-HPC)** sind ein wichtiger Ansatz für die Entwicklung führender KI-Lösungen. HPC ermöglichen in diesem Bereich durch die virtuelle Kooperation der europäischen Unternehmen unbegrenzte Computing-Ressourcen für die Unternehmen. Hier ist politische Unterstützung, insbesondere bei kartellrechtlichen Beschränkungen, erforderlich. Erste Kooperationsansätze sind in Vorbereitung. GAIA-X kann durch die Föderierung von Infrastrukturangeboten ein modulares Angebot auch von HPC-Anwendungen für unterschiedlichste Nutzer verfügbar machen.
- **Entwicklung von Next Generation Technologies und Architekturen**, wie zum Beispiel die Edge-Computing-Cloud-Architektur, ist ein vielversprechender Ansatz, der von der deutschen Industrie verfolgt wird. Deutsche Anbieter sind in diesem Segment gut aufgestellt. Mittel- bis langfristig stellt das Quantencomputing einen wichtigen Hoffnungsträger dar, um technologisch bei Cloud-Services aufzuholen. Hier besteht dringender Handlungsbedarf für Entscheidungsträger aus Politik und Wirtschaft, damit sich Deutschland und Europa auf diesem technologischen Gebiet zukünftig führend positionieren können.

Zusammenfassung

Um Abhängigkeiten von globalen Anbietern überwinden zu können, muss langfristig auf eine **Kommodifizierung** der Angebote der **Hyperscaler** hingearbeitet werden. **Europäische Projekte** wie GAIA-X Sovereign Cloud Stack und die **Gardener Cloud Foundation** können hier einen wertvollen Beitrag leisten, um die **Portabilität der Daten** über die Plattformen hinweg zu ermöglichen. Auf diese Weise kann die **Innovationsfähigkeit** Deutschlands und Europas in diesem Bereich **sichergestellt** werden.

4 Platform-as-a-Service (PaaS)

Anwendungs- und Entwicklungsökosysteme B2B und B2C (Abstraction Layer, Container Technology) QC, KI, **IoT**

Reallabor: keines
Institution: GAIA-X/Vollendung des europäischen Binnenmarkts

Elemente dieser Ebene

Die Ebene **Platform-as-a-Service (PaaS)** umfasst Anwendungs- und Entwicklungsökosysteme im B2B- und B2C-Kontext.

Deutsche und europäische Anbieter haben im **B2B-Bereich** aufgrund der industriellen **Domänenexpertise** marktführende Angebote – zum Beispiel SAP als globaler Marktführer bei ERP-Systemen, Dassault mit marktführender Rolle bei PLM-Systemen und Siemens, das mit MindSphere ein IoT-Betriebssystem hat (noch mit geringem Marktanteil). Diese europäischen Unternehmen kommen jedoch nur auf etwa zehn Prozent der Unternehmenswerte amerikanischer Firmen. Ein Grund hierfür sind **unzulängliche Skalierungsmöglichkeiten durch einen fragmentierten, heterogenen europäischen Markt.**

Im **B2C-Segment** gibt es bereits große **Abhängigkeiten** von US-Plattformanbietern wie Amazon, Facebook, Microsoft oder Google. Die starke **Marktstellung** dieser B2C-Hyperscaler wird von europäischen Anbietern auf absehbare Zeit nicht einzuholen sein. Hier ist eine wesentliche Herausforderung, wie man mit den teilweise monopolartigen Stellungen dieser Plattformen, bei denen eine Beeinflussung von politischen **(Willensbildungs-)Prozessen** nicht ausgeschlossen werden kann, aus **regulatorischer Sicht** zukünftig umgehen soll.

Aufgrund der Bedeutung von Kompetenzen für den Erhalt von Digitaler Souveränität sind Plattformen für den **Bildungs-, Wissenschafts- und Medienbereich** essenziell. Es gibt bereits Vorschläge für Bildungsplattformen, die mit Nachdruck weiterzuverfolgen sind. Auch hier müssen Agilität und Nutzerorientierung Leitlinien sein – es gilt, die privatwirtschaftliche Innovationskraft zu nutzen.

PaaS bietet für Unternehmen den Vorteil, dass sie keine **Ressourcen** für die Entwicklungsinfrastruktur einplanen müssen und vorgefertigte Softwaremodule (Micro-Services) genutzt werden können. Dies schafft **Potenziale** für den Markteintritt von **Start-ups** und erhöht die Wettbewerbsfähigkeit etablierter Unternehmen, indem Kosten gesenkt werden und die Agilität erhöht wird. Bei einem Rückgriff auf PaaS-Lösungen bestehen jedoch auch Risiken, wie zum Beispiel eine größere Gefahr von **Informationsabflüssen** oder eine potenzierte **Abhängigkeit** gegenüber dem PaaS-Anbieter.

Europäische Anbieter sind durch engere Regulierung strengeren Auflagen unterworfen als die internationalen Hyperscaler. Hier sollten **gleiche Wettbewerbsbedingungen** für europäische und internationale Anbieter gelten.

Die Forcierung eines **europäischen Wirtschafts- und Rechtsraumes und die Vollendung des einheitlichen digitalen Binnenmarktes** sind die Basis für die Skalierung von europäischen Anbietern (sowohl im B2C- als auch im B2B-Bereich). Die Erlangung der **Souveränität bei Ebene 2** (O-RAN-Initiative) und **Ebene 3** (GAIA-X-Initiative) gelten als die **Voraussetzung**, um technologisch auf **Ebene 4** (PaaS) Souveränität entwickeln zu können. Sie werden deshalb seitens der **Industrie breit unterstützt**.

Industrial IoT/I 4.0-Reallabor als EU-Pilot zur Digitalisierung der europäischen Industrie

Um den aktuell heterogenen B2B-Bereich in Europa zu vereinheitlichen und so die Digitalisierung der europäischen Industrie voranzutreiben, wird von industriellen Arbeitskreisen die Erstellung einer herstellerübergreifenden, föderierten IIoT/I 4.0-Plattform auf Basis von **standardisierten Schnittstellen** vorgeschlagen. Dabei sollte auf bestehenden Initiativen wie *GAIA-X* (Domäne Industrie), der *Plattform Industrie 4.0* und *35c*[3] und weiteren Angeboten aufgebaut und diese verstärkt werden. Zwei Hauptanwendungsfälle sollten im Fokus stehen: **Smart-Product-Angebote**, das heißt der Verkauf von Maschinen als Service, und die **Smart Factory**, also die Vernetzung aller Maschinen unterschiedlicher Hersteller innerhalb der Fabrik nach Industrie 4.0-Vorbild. Hervorzuheben ist:

- Zur **Sicherung der Konnektivität** unterstützt diese Plattform Industrie 4.0-relevante Standards (OPC/UA, LWM2M, MQTT ...) und nutzt 5G-Technologie.
- Im **Edge-Layer** kann Datenverarbeitung und -visualisierung in Echtzeit mittels KI/Maschinellem Lernen/Data Analytics stattfinden.
- Steuerung und Management der Smart Factory werden durch den **Control-Layer** abgedeckt.

Diese **Plattformbasis** sollte von einem **Konsortium** geplant und pilotiert werden. **Bestehende europäische Softwarelösungen** (zum Beispiel Siemens Mindsphere, SAP Digital Manufacturing Cloud, ADAMOS/Software AG oder Bosch IoT Suite) bilden die

3 | Vgl. BMWi 2020.

jeweils eigenständige Vermarktungsbasis, wobei die Schnittstellen in Open-Source als **gemeinsame Konnektivität** weiterentwickelt und integriert werden.

Durch eine gemeinsam abgestimmte Entwicklung kann die europäische Plattformlandschaft **defragmentiert** werden, was zu **erheblichen Skaleneffekten** und einer **stark verkürzten Markteinführungszeit** für die **Digitalisierung der europäischen Industrie** führt. Auf diese Weise können die nationalen und europäischen **Digitalisierungsstrategien für Industrie und Mittelstand/KMU entscheidend beschleunigt** werden. In diesem Kontext gilt es, eine **Innovations- und Start-up-Kultur** (inklusive Kapital) zu **fördern**, welche eigene nutzerorientierte Angebote agil und modern entwickelt.

Gleichzeitig wird durch die Etablierung eines in **Europa ansässigen IIoT-Architekturstandards** die **Digitale Souveränität** der europäischen Industrie **gesichert**. Hier **können europäische Kompetenzen im Bereich der Telekommunikation** (Deutsche Telekom, Ericsson, Nokia) eingesetzt und mit dem **industriellen Know-how** der europäischen Technologieführer **verknüpft** werden.

Zusammenfassung

Dieser Ebene kommt eine zentrale Bedeutung für Innnovationen, die auf Ebene 5 beziehungsweise 6 entwickelt werden, zu, da die **Verfügbarkeit entsprechender Services für die Skalierung neuer Geschäftsmodelle entscheidend** ist. Im **B2C-Bereich** sind bereits **starke US-Plattformen** entstanden. Hier gilt es den entstandenen Abhängigkeiten politisch sowie regulatorisch zu begegnen.

Im **B2B-Bereich** gibt es **bislang keine dominierenden Plattformen** und zahlreiche Industrien beginnen gerade erst mit der Digitalisierung. Um die Zukunftsfähigkeit und Industrie 4.0-Führerschaft (und damit auch Souveränität) Deutschlands und Europas zu sichern, **müssen** innovative domänenspezifische Plattformen und Geschäftsmodelle **jetzt und hier entstehen**. Aktuell sind vorhandene europäische Angebote zu fragmentiert, deshalb ist die **Etablierung einer kollaborativen IIoT-Plattform** eine wichtige Voraussetzung zur Sicherung der Souveränität der europäischen Industrie. Ein **kollaboratives Reallabor** zu deren Umsetzung sollte daher breite Unterstützung aus Industrie, Wirtschaft und Politik erfahren.

5 Europäische Datenräume

Zum Beispiel für **Mobilität**, Health, Public Sector, digitaler öffentlicher Raum

Reallabor: Datenraum Mobilität Institution: GAIA-X, Datenstrategie D, EU

Elemente dieser Ebene

Im digitalen Zeitalter sind **Daten mehr denn je eine Schlüsselressource für Wirtschaft, Wissenschaft und Gesellschaft**. Die Fähigkeit, Daten zu nutzen, zu verknüpfen und auszuwerten, ist gleichermaßen Grundlage für Innovation und wirtschaftliche Prosperität, für das Generieren von Wissen und für den gesellschaftlichen Zusammenhalt.

Trotz dieser immensen Chancen und trotz fortschreitender Digitalisierung **schöpft Deutschland das enorme Potenzial der erhobenen Daten** für Wirtschaft, Wissenschaft und Gesellschaft – und auch für Digitale Souveränität – bei Weitem **nicht aus**. Die Gründe dafür sind zahlreich – von fehlenden Standards über Unsicherheiten des rechtlichen Rahmens bis hin zum fehlenden Willen, Daten zu teilen.

Die digitale Ökonomie ist eine **datenfokussierte Ökonomie**. Insbesondere Anwendungen, die **Künstliche Intelligenz** (KI) nutzen, sind von großen **Datenmengen** vollständig **abhängig**, um Datenmuster zu erkennen und daraus Algorithmen zu entwickeln. Deshalb muss es das Ziel sein, große vernetzte, offene und sichere Datenräume in Europa zu erzeugen.

Im **B2C-Bereich** sind diese Datenräume in den USA und in China entstanden – deutschen beziehungsweise europäischen Firmen fehlen in diesen Bereichen bereits die Daten für Innovationen. Außerdem ergeben sich – aufgrund der **Kontrolle über Datenräume** europäischer Daten außerhalb Europas – Souveränitätsfragen. Um diesen zu begegnen, ist entscheidend, die **Regulationshoheit** (Stichwort: US **CLOUD Act** hinsichtlich des **Datenzugangs**, zu dem eine **europäische Antwort noch fehlt,** beziehungsweise **Digital Service Act hinsichtlich der Content Regulation**) und **Governance-Hoheit** (Stichwort: Durchsetzen von europäischen (DSGVO-)Standards gegenüber Anbietern) zu behalten.

Im **B2B-Bereich** sind solche **Datenräume größtenteils noch nicht entstanden**. Sollte es amerikanischen und chinesischen Hyperscalern gelingen, auch hier die maßgeblichen Datenräume zu errichten beziehungsweise zu beherrschen, hätte dies gravierende wirtschaftliche Folgen für Deutschland und Europa und bedeutete in der Konsequenz dann auch Einschränkungen des Handlungsspielraumes und somit der Souveränität.

Die **Entwicklung** und schnelle **Umsetzung** attraktiver Angebote für industrielle **Datenökosysteme** und hoheitliche Aufgaben muss daher **politisch begleitet** und gefördert werden. Initiativen wie **GAIA-X** und die **International Data Spaces** (IDS) stellen hierfür wichtige **politische Ausgangspunkte** und **konzeptionelle Blaupausen** dar. In verschiedenen Papieren des Bundes und Europas wurde die Bedeutung von **vertrauenswürdigen Datenräumen**, die einen sicheren domänenspezifischen und -übergreifenden Datenzugang beziehungsweise -austausch ermöglichen, bereits erkannt. Die am 27.01.2021 veröffentlichte Datenstrategie des Bundes[4] ist ein wichtiges Instrument und sollte konsequent umgesetzt werden.

Beispiel Datenraum Mobilität – Problemstellung und Status quo

Zur Erreichung der Datensouveränität in Deutschland und Europa besteht im Mobilitätsbereich ein großer **Bedarf** an der **Vernetzung heterogener Daten** und **Dienste**, um eine nutzerfreundliche und nachhaltige Mobilität der Zukunft – zum Beispiel die Verknüpfung verschiedener Verkehrsträger zu einer intermodalen Reisekette – zu ermöglichen.

Der große Wert einer Vernetzung von Daten in einem Datenraum besteht darin, dass neue Mobilitätsdienste und **komplementäre Geschäftsmodelle** (B2B und B2C) realisiert werden können.

Dabei sind zwei grundlegende Voraussetzungen zu schaffen:

1. Das Erreichen des **Commitments aller relevanten Stakeholder**, Daten zu liefern, als Voraussetzung für die erfolgreiche Implementierung des Datenraums. Hier wurde schon seit einigen Jahren erfolglos versucht, solch ein Commitment zu erlangen.

2. Ein **regulatorisch** und **industriepolitisch definierter Rahmen** muss entwickelt werden, damit nicht als Ergebnis der Schaffung des Datenraumes lediglich die Hyperscaler noch schneller ihre Dominanz ausbauen können, sondern die neuen, oft Start-up-getriebenen Aktivitäten in Europa eine Chance haben.

4 | Vgl. Bundeskanzleramt 2021.

Lösungsansatz und Ziele

Orientiert an europäischen Werten soll ein **vertrauenswürdiger, sicherer und dezentral vernetzter Datenraum Mobilität (DRM)** etabliert werden, um damit ein wettbewerbsbelebendes Marktumfeld und ein **Common Level Playing Field** zu garantieren (siehe Abbildung 5).

Der DRM zielt darauf ab, beteiligten Anwendern eine beschleunigte **Umsetzung** innovativer **daten- und KI-basierter Mobilitätsangebote** zu erlauben und ihnen die Chance zu geben, ohne Dominanz außereuropäischer Hyperscaler vom Start weg erfolgreich zu sein.

Gemeinsame Nutzungsregeln und vertrauensvolle Datenstandards, Zugangsrechte und Pflichten auf Basis **europäischer Werte** müssen gewährleistet sein. Die **Datenbereitstellung** erfolgt dabei **freiwillig**. Auch KMU, Start-ups sowie Forschungs- und Entwicklungsprojekte sollen den DRM für ihre Zwecke nutzen können.

Die derzeitige Projektarbeit konzentriert sich auf **drei zentrale Punkte**:

1. Konkrete Ausgestaltung einer an **europäischen Werten** orientierten **Governance und Design des Geschäftsmodells**
2. Definition der DRM-spezifischen **technologischen Anforderungen**
3. Ausrichtung der Markteinführung, Europäisierung und Skalierung des Datenraum

Der DRM ermöglicht als „**Datendrehscheibe**" den Datenaustausch. Unterschiedliche Sub-Datenräume werden über Konnektoren dezentral miteinander vernetzt. Diese Konnektoren gewährleisten dabei die sichere Dateninteraktion.

Der **Mobilitäts Daten Marktplatz (MDM)** beziehungsweise der Nationale Zugangspunkt für Mobilitätsdaten ist ein zentraler Sub-Datenraum für den DRM. Darin sind unter anderem statische und dynamische Reise- und Verkehrsdaten, Daten der öffentlichen Verkehrsbetriebe und Routenpläne enthalten. Im DRM werden Daten und Dienste der Stakeholder auf freiwilliger Basis vernetzt: zum Beispiel Fahrzeug-, Infrastruktur- und Wetterdaten sowie Informationen zu Baustellen und Großstörungen.

Die **Referenzarchitektur** des **IDS** dient als Grundlage für Dateninfrastruktur und Systemarchitektur. Dadurch ist auch die **Anbindung** an **GAIA-X** gewährleistet. Der IDS stellt die Datensouveränität der einzelnen Datengeber sicher, da Nutzungsbedingungen an die Datenlieferung gekoppelt werden können. Identifikation, Authentifizierung sowie Datenschutz sind garantiert.

Das **Commitment** der **Datenanbieter** und **-nutzer** ist für das Projekt erfolgskritisch. Derzeit wird mit einer repräsentativen Gruppe von Akteuren (private und öffentliche Mobilitätsdienstleister, OEMs, Plattformkonzerne und Digitalwirtschaft) gestartet. Durch die Klärung des politischen und rechtlichen Rahmens und das Aufsetzen des Gesamtkonzepts des DRM werden die Grundlagen der Zusammenarbeit definiert – mit dem Ziel, einen Sogeffekt auf weitere mobilitätsrelevante Akteure auszulösen.

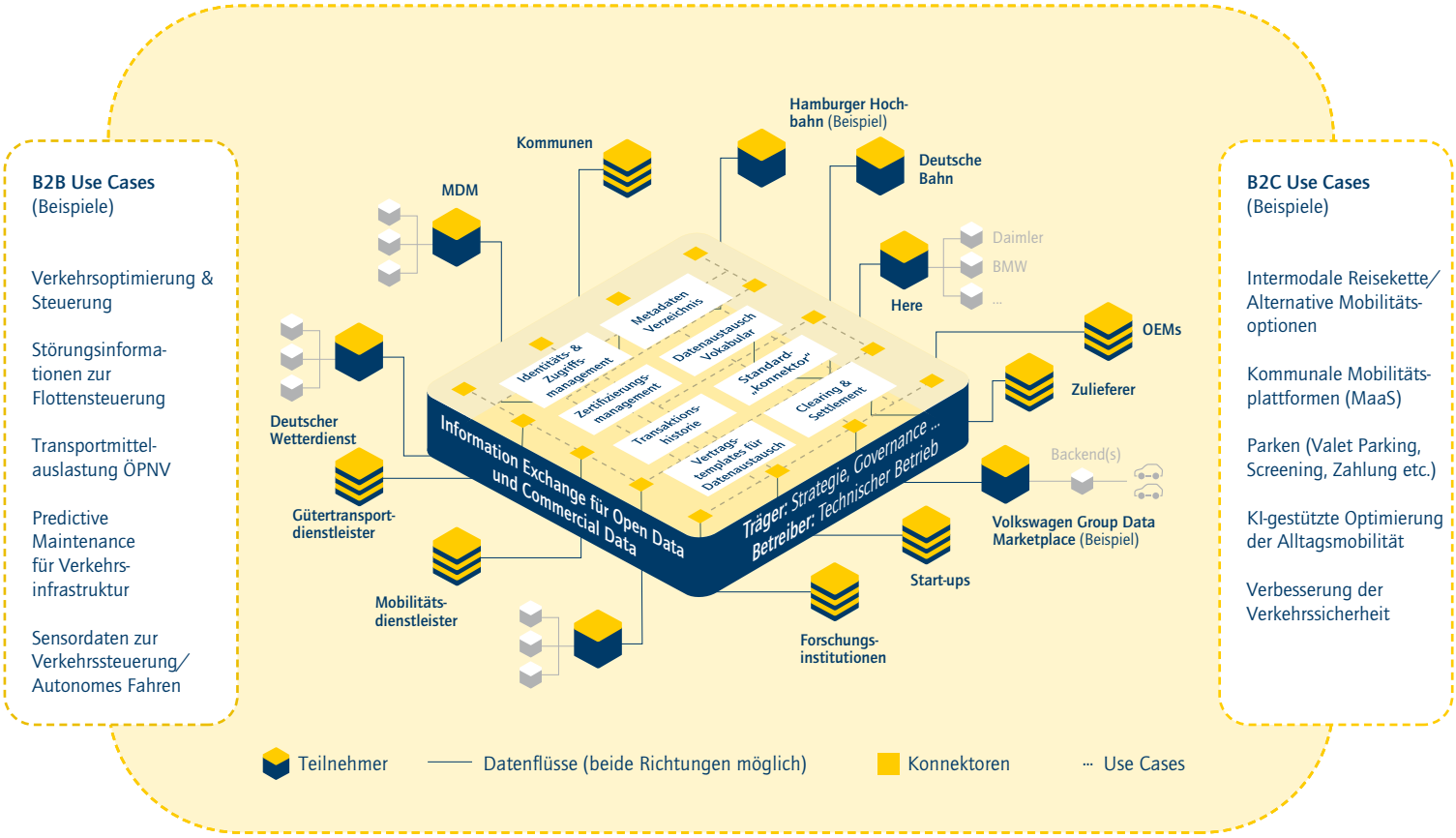


Abbildung 5: Exemplarische Darstellung: dezentral vernetzter Datenraum Mobilität (Quelle: DRM 2021)

Zusammenfassung

Vertrauenswürdige **Datenräume**, die eine **sichere domänenspezifische** und -**übergreifende Dateninteraktion** ermöglichen, sind für die Umsetzung von datengetriebenen und plattformbasierten Geschäftsmodellen der Zukunft essenziell. Mit dem **Datenraum Mobilität** haben sich die Bundesregierung sowie private und öffentliche Mobilitätsanbieter zum Ziel gesetzt, bis Ende 2021 ein umfassendes Datennetzwerk Mobilität zu schaffen, das verschiedene Sub-Datenräume vernetzt und die Datensouveränität der Akteure sicherstellt. Die **verantwortungsvolle Datennutzung** politisch zu fördern und zu begleiten ist wesentlich für den Erfolg in der digitalen Ökonomie. Die Verabschiedung der Datenstrategie mit Blick auf Innovation ist ein wichtiger Rahmen dafür.

6 Softwaretechnologien

App-Entwicklungen, Office, ERP, KI, Middleware, Robotik-Software, Blockchain, Algorithmen, **EU-Open Source,** VR/AR, QC

Reallabor: keines
Institution: Agentur für Sprunginnovation, KI-Verbund

Elemente dieser Ebene

Der Zugang zu App-Entwicklungstools, ERP-Systemen, zu Middleware und auch zu Software für Robotik und Blockchain/Distributed Ledger Technologies ist durch **europäische Entwickler und Anbieter** sowie ein breites **internationales Angebot weitgehend unkritisch**. Allerdings bestehen nach Einführung entsprechender Systeme für die jeweilige Organisation Abhängigkeiten zum jeweiligen Produkt.

Erhebliche Abhängigkeiten bestehen bei **Betriebssystemen (Windows, iOS, Android)** sowie **Microsoft Office**. Diese stellen für viele Privatpersonen, Unternehmen und Verwaltungen den De-facto-Standard dar. Die Bindung an die Ökosysteme der Anbieter wird durch eine **zunehmende Abhängigkeit** der Funktionalitäten von **Onlinediensten der Anbieter** weiter verstärkt, beispielsweise im Rahmen der Umstellung auf das Microsoft-365-Cloud-Servicemodell.

Ähnlich wie bei ERP-Systemen europäischer Anbieter ist ein Wechsel zu Alternativanbietern nur mit sehr hohen Aufwänden möglich. Diese können in einer Extremsituation als Verhandlungsoption genutzt werden, falls der Zugang zu Windows und Office eingeschränkt zu werden droht. Insgesamt sollten Abhängigkeiten jedoch reduziert werden.

Der fokussierte Einsatz von Open Source kann in ausgewählten Bereichen einen Beitrag zur Reduktion von Abhängigkeiten und zu mehr digitaler Souveränität im Softwarebereich leisten. Dem öffentlichen Sektor kommt hier eine wesentliche Rolle zu, um Innovation in diesem Bereich wie auch die entsprechende Community zu stärken. Dabei sollten Fehler der Vergangenheit vermieden werden: Wichtig wären ein strategischer **Fokus auf Reduzierung von Abhängigkeiten** sowie die **Schaffung offener und föderierbarer Plattformen**, welche die Basis für Start-ups und eine schnell wachsende europäische Digitalindustrie bilden können, die konkrete Anwendungen mit Kundennutzen generiert. Als Anknüpfungspunkte für weitere Prüfungen könnten dienen:

- Erwägung eines gezielten Einsatzes von Open-Source-Software bei der **Digitalisierung von Staat und Verwaltung** durch strategische Ausrichtung der Vergabeverfahren und Förderung auf Open-Source-Lösungen
- Nutzung von **Open-Source-Hardwarekomponenten** und Open-Source-Software für den **Betrieb hochsensibler Bereiche**
- **Schaffung** (über Vergabeverfahren) und **Förderung** (mit sehr konkreten Zielvorgaben) von **Open-Source-Software und Plattformen**
- Schaffung von **Standards** (Schnittstellen, Sicherheitslevel, Libraries), um eine hohe Wiederverwendung von Bestandteilen über Behörden hinweg zu ermöglichen
- **Unterstützung von Initiativen** wie der Open Source Business Alliance e. V., der Gardener Cloud Foundation oder der Eclipse Foundation auf europäischer Ebene

Bei entsprechenden Initiativen sollte **aus vergangenen Umstellungsversuchen gelernt** werden, da in der Vergangenheit viele Projekte an dem Ansatz, Softwareentwicklung am Markt vorbei und direkt aus Behörden heraus zu betreiben, gescheitert sind, während von Unternehmen entwickelte und häufig „nicht sichtbare" Open-Source-Software im Server- oder Applikationsbereich in Städten, Ländern und Bund bereits heute sehr erfolgreich eingesetzt wird.

Für **europäische Software-Start-ups** besteht die **Chance, hier innovative Produkte anzubieten**. Allerdings sind sie darauf angewiesen, dass ein **Common Level Playing Field** mit den internationalen Wettbewerbern unter Berücksichtigung des europäischen Rechtsrahmens gesichert wird. Die Durchsetzung von Governancehoheit gegenüber Anbietern, welche diesem Rechtsrahmen nicht entsprechen, **sollte forciert werden**.

Auch mit **Open-Source-Software** können **Fragen Digitaler Souveränität** verbunden sein, weil Teile der Open-Source-Software und ihrer Communities von kommerziellen Anbietern abhängig sind und Entwicklungen im Open-Source-Bereich nicht immer allen als digitales Gemeingut zur Verfügung stehen.

So erfreut sich beispielsweise die von **Google** bereitgestellte Programmbibliothek **TensorFlow** großer Beliebtheit bei der **KI-Entwicklung**. Google bindet die Entwicklergemeinde durch dieses Angebot näher an sich und sein Ökosystem und erhält früh Einblicke in Trends und Anwendungsgebiete. Neben der Förderung von Open-Source-Software und Plattformen ist deswegen der Aufbau von Wissen über Open-Source-Entwicklungs- und Lizenzmodelle sowie über die Funktionsweise von Open

Source Communities wichtiger Faktor für die Erlangung digitaler Souveränität.

Auch die **geografische Verteilung von Entwicklergemeinden**, **Abhängigkeiten von proprietären Betriebssystemen** (gerade bei Smartphones auch vom damit verknüpften Ökosystem und den Geschäftsmodellen) und Softwarebestandteilen sowie Standards und Normen sind wichtige Faktoren bei der Bestimmung des Grades Digitaler Souveränität und strategischer Handlungsoptionen im Open-Source-Bereich.

Zusammenfassung

Grundsätzlich besteht bei dieser Ebene **Handlungsbedarf**, weil es signifikante **Abhängigkeiten** von amerikanischen Anbietern im **OS- und Office-Bereich** gibt, die gezielt genutzt werden, um neue Abhängigkeiten zu den Cloud-Angeboten der betreffenden Anbieter zu schaffen. Der öffentlichen Hand fällt bei deren Reduzierung eine zentrale Rolle zu.

Open Source hat das strategische Potenzial, Digitale Souveränität zu stärken und Innovation zu fördern, ist allerdings **kein Selbstläufer**.

Über **gezielte, strategisch abgeleitete Vergabestrategien** kann die bestehende Open-Source-Community gestärkt und die **Entstehung nutzbarer digitaler Gemeingüter** gefördert werden. Der öffentliche Sektor und seine Dienstleister können über Community-Arbeit die weltweite Open-Source-Community fördern, was wiederum strategische Unabhängigkeit von einzelnen Firmen bedeutet. **Ein gemeinsames Security Framework** des öffentlichen Sektors kann den Einsatz und die Wiederverwendbarkeit von Open Source fördern und das Teilen von Open Source zwischen den Behörden ermöglichen. Bei Initiativen und der Förderung dieses Bereichs ist stets eine umfassende **Analyse der formalen und informellen Strukturen** der betreffenden Open-Source-Ökosysteme angeraten.

7 Europäisches Rechts- und Wertesystem

Cybersecurity, Kryptografie, **E-Identity,** EU-Zertifizierung (Verbraucherschutz) und Standards

Reallabor: Cybersecurity Center
Institution: BSI + Netzwerk Cyberregionen in D

Elemente dieser Ebene

Hinsichtlich Digitaler Souveränität ist die entscheidende Frage auf dieser Ebene, inwiefern es gelingt, **europäische Grundüberzeugungen** und Werte **in konkrete Spielregeln für den europäischen Binnenmarkt** zu übersetzen, an die sich dann auch alle – egal ob europäische, amerikanische oder asiatische – **Unternehmen, ihre Dienstleistungen und Produkte** (Value by Design) halten müssen.

Dabei kann das erfolgreiche **Umsetzen von Value by Design** innovative Produkte und Dienstleistungen mit einem entsprechenden **Konkurrenzvorteil** hervorbringen und wirtschaftliches Wachstum bedeuten. Eine prosperierende digitale Ökonomie ist wiederum ein Stabilitäts- und Souveränitätstreiber.

Mit der zunehmenden Digitalisierung („alles ist mit allem verknüpft") werden auch Cyberangriffe zunehmen („alles wird gehackt"). Die **Fähigkeit, Cyberangriffe abzuwehren, ist essenziell** und kann an Bedeutung nicht überbetont werden. Dabei geht es letztlich um Angriffe über alle Ebenen des Schichtenmodells hinweg; zunehmend auch durch autokratische Systeme, die eben **jene Werte** beziehungsweise die Durchsetzung der auf ihnen basierenden **Wirtschafts- und Rechtsordnung angreifen.**

Entsprechend der in diesem Papier eingenommenen Technologieperspektive braucht es eine **souveräne Kontrolle** über die **für Cybersecurity zentralen Technologien** und die **technischen und organisationalen Infrastrukturen ihrer Anwendung**.

Fokusbereich Cybersicherheit – Status quo

Zusammenfassend lässt sich sagen, dass es **Deutschland und Europa** nicht an Technologien oder Akteuren mit dem notwendigen Sachverstand mangelt, wenn es um Cybersicherheit geht. Was **fehlt**, ist eine **effektive europäische Koordinierung der vorhandenen Kräfte**.

Denn Europa und insbesondere **Deutschland** sind in der **Erforschung und Entwicklung von Cybersecurity-Technologien stark** aufgestellt. Dies beginnt bei der **kryptografischen Forschung** und reicht bis hin zu **FinTech-Start-ups** wie Fraugster und Risk.Ident, die KI-basierte, skalierbare Softwarelösungen entwickeln, um Menschen und Organisationen vor Identitätsdiebstahl, Kontofälschung oder Accountübernahme zu schützen.

Auch kompetente Organisationen existieren bereits. Mit dem **Bundesamt für Sicherheit in der Informationstechnik (BSI)** wurde eine staatliche Stelle geschaffen und ausgebaut, die für die Prävention und Detektion von Cyberangriffen sowie für die **Reaktion auf diese** verantwortlich ist. Über die Allianz für Cybersicherheit wird versucht, die Widerstandsfähigkeit des Standorts in Summe zu stärken. Die **Bundesdruckerei (BDr)** ist bei der technischen Entwicklung von **Sicherheitslösungen** und dafür nötiger Infrastrukturen ein führender und hochinnovativer Akteur in Staatsbesitz.

Aufmerksamkeit für Cybersicherheit besteht ebenfalls in der Wirtschaft. Wege zur **Vermeidung steigender digitaler Verwundbarkeiten** im Zuge der engeren Vernetzung der **industriellen Produktion** werden zum Beispiel von der Plattform Industrie 4.0 in den Arbeitsgruppen „Sicherheit vernetzter Systeme" und „Rechtliche Rahmenbedingungen" erarbeitet. Es gibt **inzwischen etliche Initiativen**, die dafür sorgen, dass Angriffsvektoren schnell und vertrauensvoll geteilt werden, wie zum Beispiel die DCSO (Deutsche Cyber-Sicherheitsorganisation).

Die technische **Kompetenz** für die **Bewertung der Sicherheit** und für die Zertifizierung komplexer Systeme, insbesondere von **ausländischen Herstellern**, ist **prinzipiell vorhanden**. Solche Vorhaben **scheitern aber oftmals** an einer fehlenden Offenlegung der dafür nötigen Unterlagen beziehungsweise dem umfassenden Zugriff auf die Systeme. Diesen zu ermöglichen, ist eine **politische Herausforderung**.

Lösungsansatz

Eine Harmonisierung der heterogenen Cybersicherheitslandschaft Deutschlands und Europas muss politisch vorangetrieben werden. Mit dem **Cybersecurity Act** (einer EU-Verordnung, die unter anderem neue Richtlinien und eine einheitliche Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik einführt), der Richtlinie zur Netz- und Informationssicherheit (**NIS-Richtlinie**) sowie der **europäischen Datenstrategie** wurden hierzu bereits wichtige Schritte unternommen.

Eine engere Kooperation staatlicher Stellen der EU-Mitgliedsstaaten und der **Europäischen Agentur für Cyber-Sicherheit (ENISA)** sollte ebenfalls institutionalisiert werden.

Im Rahmen gemeinsamer Anstrengungen sollten vor allem in den folgenden drei Bereichen die **Weiterentwicklung und flächen-**

deckende Implementierung folgender **Cybersecurity-Ansätze** verfolgt werden:

- **Verschlüsselungstechnologien**: Die kontinuierliche Erforschung **kryptografischer Grundlagen,** die Entwicklung **starker Verschlüsselungsverfahren** inklusive der Post-Quanten-Kryptografie und die Förderung einer flächendeckenden **Nutzung**, zum Beispiel durch Zertifizierungen und in kritischen Bereichen durch vorgeschriebene Mindeststandards, durch die und innerhalb der EU haben höchste Priorität. Darüber hinaus sind noch existierende Zertifizierungslücken (insbesondere für Komponenten) zu schließen.
  In diesem Bereich kann **Digitale Souveränität** nicht durch den Zugang zu einem externen Anbieter erreicht werden, sondern **nur durch eigene umfassende Kompetenzen**. Auch wenn bestimmte starke Verfahren aus politischen Gründen in kommerziellen Produkten dann nicht zum Einsatz kommen, muss stets die Verfügbarkeit der modernsten Verfahren sichergestellt bleiben.
- **Institutionalisierte Abwehrfähigkeiten**: Gerade **KMU** sind oft nicht in der Lage, aus eigener Kraft Cybersecurity-Vorkehrungen auf höchstem Niveau zu treffen. Sie sind **auf Sensibilisierung**, die **Vermittlung von Kenntnissen** und **rasche externe Hilfe** im Krisenfall **angewiesen**.
  Hier gilt es das Angebot **an öffentlichen Beratungsangeboten** auszubauen und **privatwirtschaftliche Cyber Defence Center** oder Kollaborationsorganisation als wichtige Bestandteile des **Cybersecurity-Ökosystems** zu begreifen, die Erfahrungen zusammentragen und durch Kostensynergien und die Bündelung von Informationen Angriffen wirtschaftlich begegnen können.
  Dies setzt eine **klare Arbeitsteilung** zwischen den **öffentlichen und den gewerblichen Akteuren** voraus, damit beide weder in Konkurrenz zueinander geraten, was die Geschäftsmodelle der privatwirtschaftlichen Akteure bedrohen würde, noch Lücken im Monitoring von Bedrohungslagen und ihrer effektiven Bekämpfung entstehen.
- **E-Identity**: Für den vertrauensvollen Austausch von Daten und ein sicheres Agieren in digitalen Räumen sind **fälschungssichere digitale Identitäten** unerlässlich.
  Von zentraler Bedeutung ist, dass die Personenidentitäten nutzerzentriert und **leicht durch Bürgerinnen und Bürger bedienbar** entwickelt werden. Aktuell hat sich keine europäische Lösung am Markt etabliert. Die Vernetzung existierender europäischer Identity-Provider, wie zum Beispiel der Bundesdruckerei, zur Entwicklung einer europäischen e-ID-Lösung könnte ein Weg sein, eine solche einfache Nutzung digitaler Dienste – und bei richtiger Ausgestaltung auch eine **volle Kontrolle über die Daten** – zu erlauben.
  Nicht nur Menschen, auch **Maschinen brauchen eindeutige Identifizierbarkeit**, wenn sie im Rahmen von Industrie 4.0 und IoT ihr volles Potenzial entfalten sollten. Hier sind mit Hochdruck Lösungen zu entwickeln.
  All dies macht nur im Rahmen eines **interoperablen europäischen ID-Ökosystems** Sinn, da **sonst kein ausreichendes internationales Gewicht** erreicht werden kann, um Standards von weltweiter Bedeutung zu setzen, an denen und den darin verankerten Werten sich Hersteller orientieren. Dabei kann auf dem bestehenden europäischen **eIDAS-Ökosystem** (electronic IDentification, Authentication and Trust Services) hoheitlicher digitaler Identitäten aufgebaut werden.
  Daher ist der von der Bundesregierung und Unternehmen gemeinsam angestoßene Aufbau eines Ökosystems digitaler Identitäten der richtige Schritt und dringend geboten. Er wird aber nur erfolgreich sein, wenn es gelingt, die **EU-Kommission** und eine **kritische Masse an Mitgliedsstaaten** ebenfalls hinter dieser Initiative zu versammeln.

Zusammenfassung

Digital souverän ist im Bereich **Cybersicherheit** nur, wer das gesamte Spektrum von der Grundlagenforschung bis hin zur Implementierung beherrscht. Dies ist in Europa der Fall und sollte aufrechterhalten werden. Nur auf dieser technologischen Basis kann für die Wirtschaft und die europäische Gesellschaft ein souveränes Agieren im digitalen Raum **auf Basis europäischer Wertevorstellungen** sichergestellt werden. Verwirklicht werden kann dies dann **nur im Rahmen des europäischen Binnenmarkts**, da nur dieser ein ausreichendes internationales Gewicht aufweist, um erfolgreich entsprechende Standards zu setzen.

Literatur

BMWi 2020
Bundesministerium für Wirtschaft und Energie: *Eckpunkte zur Umsetzung des Konjunkturpakets Ziffer 35c. Zukunftsinvestitionen Fahrzeughersteller und Zulieferindustrie sowie Forschung und Entwicklung*, Berlin 2020.

Buchenau et al. 2021
Buchenau, M./Koch, M./Tyborskim R.: *Wirtschaft und Wissenschaft fordern Quantencomputer binnen fünf Jahren*, 2021. URL: https://www.handelsblatt.com/technik/it-internet/druck-auf-bundesregierung-wirtschaft-und-wissenschaft-fordern-quantencomputer-binnen-fuenf-jahren/26796470.html [Stand:19.02.2021].

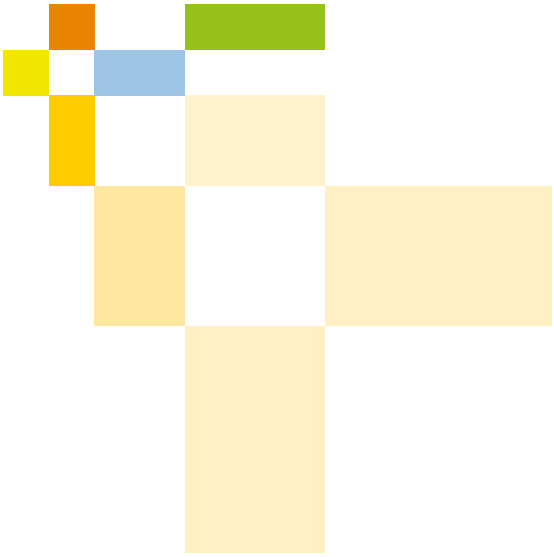
Bundeskanzleramt 2021
Bundeskanzleramt: *Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum*, Berlin 2021.

DRM 2021
Datenraum Mobilität: *Dezentral vernetzter Datenraum Mobilität* [unveröffentlichtes Manuskript], 2021.

Kagermann et al. 2020
Kagermann, H./Süssenguth, F./Körner, J./Liepold, A.: *Innovationspotenziale der Quantentechnologien der zweiten Generation* (acatech IMPULS), München 2020.

SAP 2021
SAP: *Gardener – ein offener, kohärenter und erweiterbarer Standard* [unveröffentlichtes Manuskript], 2021.

Telefonica 2020
Telefónica Deutschland: *Die Vorteile der Open-RAN-Architektur*, 2020. URL: https://www.basecamp.digital/mobilfunk-fuer-dummies-die-vorteile-der-open-ran-architektur/ [Stand: 19.02.2021].



acatech – Deutsche Akademie der Technikwissenschaften

acatech berät Politik und Gesellschaft, unterstützt die innovationspolitische Willensbildung und vertritt die Technikwissenschaften international. Ihren von Bund und Ländern erteilten Beratungsauftrag erfüllt die Akademie unabhängig, wissenschaftsbasiert und gemeinwohlorientiert. acatech verdeutlicht Chancen und Risiken technologischer Entwicklungen und setzt sich dafür ein, dass aus Ideen Innovationen und aus Innovationen Wohlstand, Wohlfahrt und Lebensqualität erwachsen. acatech bringt Wissenschaft und Wirtschaft zusammen. Die Mitglieder der Akademie sind herausragende Wissenschaftlerinnen und Wissenschaftler aus den Ingenieur- und den Naturwissenschaften, der Medizin sowie aus den Geistes- und Sozialwissenschaften. Die Senatorinnen und Senatoren sind Persönlichkeiten aus technologieorientierten Unternehmen und Vereinigungen sowie den großen Wissenschaftsorganisationen. Neben dem acatech FORUM in München als Hauptsitz unterhält acatech Büros in Berlin und Brüssel.

Weitere Informationen unter www.acatech.de.

Autoren:

Prof. Dr. Henning Kagermann
acatech – Deutsche Akademie der Technikwissenschaften
Karolinenplatz 4
80333 München

Karl-Heinz Streibich
acatech – Deutsche Akademie der Technikwissenschaften
Pariser Platz 4a
10117 Berlin

Dr. Katrin Suder
TAE Advisory & Sparring GmbH
Eppendorfer Landstraße 46
20249 Hamburg

Reihenherausgeber:

acatech – Deutsche Akademie der Technikwissenschaften, 2021

Geschäftsstelle
Karolinenplatz 4
80333 München
T +49 (0)89/52 03 09-0
F +49 (0)89/52 03 09-900

Hauptstadtbüro
Pariser Platz 4a
10117 Berlin
T +49 (0)30/2 06 30 96-0
F +49 (0)30/2 06 30 96-11

Brüssel-Büro
Rue d'Egmont/Egmontstraat 13
1000 Brüssel (Belgien)
T +32 (0)2/2 13 81-80
F +32 (0)2/2 13 81-89

info@acatech.de
www.acatech.de

Vorstand i. S.v. § 26 BGB: Karl-Heinz Streibich, Prof. Dr.-Ing. Johann-Dietrich Wörner, Prof. Dr.-Ing. Jürgen Gausemeier, Prof. Dr. Reinhard F. Hüttl (Amt ruht derzeit), Dr. Stefan Oschmann, Dr.-Ing. Reinhard Ploss, Prof. Dr. Christoph M. Schmidt, Prof. Dr.-Ing. Thomas Weber, Manfred Rauhmeier, Prof. Dr. Martina Schraudner

Empfohlene Zitierweise:
Kagermann, H./ Streibich, K.-H./Suder, K.: *Digitale Souveränität – Status quo und Handlungsfelder* (acatech IMPULS), München 2021.

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Koordination und Redaktion: Florian Süssenguth, Dr. Johannes Winter
Lektorat: Lektorat Berlin
Layout-Konzeption und Konvertierung: GROOTHUIS. Gesellschaft der Ideen und Passionen mbH für Kommunikation und Medien, Marketing und Gestaltung; groothuis.de
Titelfoto: © shutterstock/Vladimir Vihrev

Die Originalfassung der Publikation ist verfügbar auf www.acatech.de

Digitale Souveränität ist eine der entscheidenden politischen Zukunftsfragen. Mit jedem neuen Bereich des privaten, wirtschaftlichen und öffentlichen Lebens, in dem digitale Plattformen und Anwendungen genutzt werden, wird die Souveränität in der Nutzung entscheidender. Digitale Souveränität ist nicht nur eine Frage der Wettbewerbsfähigkeit, sondern auch der politischen Selbstbestimmtheit der Europäischen Union und ihrer Mitgliedsstaaten, der Innovationskraft von Unternehmen sowie der Freiheit der Forschungseinrichtungen und aller Europäer in der digitalen Welt.

Dieser acatech IMPULS stellt ein Schichtenmodell vor, das zu einer Konkretisierung des Konzepts der Digitalen Souveränität und vor allem zur Entwicklung konkreter Handlungsoptionen entlang der sie prägenden und aufeinander aufbauenden technologischen Ebenen beitragen soll.